

J01P0364 US00

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出 願 年 月 日

Date of Application:

2000年 8月23日

出 願 番 号

Application Number:

特願2000-252804

出 願 人

Applicant(s):

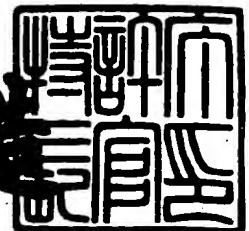
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年12月22日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 0000612902

【提出日】 平成12年 8月29日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 市村 元

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100086841

    【弁理士】

    【氏名又は名称】 脇 篤夫

【代理人】

    【識別番号】 100114122

    【弁理士】

    【氏名又は名称】 鈴木 伸夫

【手数料の表示】

    【予納台帳番号】 014650

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9710074

【包括委任状番号】 0007553

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ送出装置、データ送出方法

【特許請求の範囲】

【請求項 1】 主データと付加データとが配される複数のデータブロックを連続的に送出することで、一連の主データ及び上記一連の主データに係る付加データを送出するデータ送出装置において、

上記付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入する付加データ挿入手段と、

上記付加データ挿入手段での付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化された連続するデータブロックを送出する送出手段と、

を備えたことを特徴とするデータ送出装置。

【請求項 2】 上記データブロックの一部に乱数データを挿入する乱数データ挿入手段をさらに備え、

上記暗号化手段は、上記付加データ挿入手段での付加データ挿入処理、及び上記乱数データ挿入手段での乱数データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行うことを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 3】 上記付加データ挿入手段は、暗号化されていない付加データを、ランダムに選択したデータブロックに挿入することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 4】 上記付加データ挿入手段は、暗号化されていない付加データ、及び暗号化されている付加データを、ランダムに選択したデータブロックに挿入することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 5】 上記乱数データ挿入手段は、データブロック内における無効データ部分に、上記乱数データを挿入することを特徴とする請求項 2 に記載のデータ送出装置。

【請求項 6】 上記送出手段は、有線又は無線で接続された他の機器に対して上記連続したデータブロックを送出することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 7】 上記送出手段は、上記連続したデータブロックを記録媒体に記録するデータとして送 out することを特徴とする請求項 1 に記載のデータ送出装置。

【請求項 8】 主データと付加データとが配される複数のデータブロックを連続的に送 out することで、一連の主データ及び上記一連の主データに係る付加データを送 out するデータ送出方法において、

上記付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入し、

付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行ない、

暗号化された連続するデータブロックを送 out することを特徴とするデータ送出方法。

【請求項 9】 上記データブロックの一部に乱数データを挿入する乱数データ挿入処理が行われ、

上記付加データ挿入処理、及び上記乱数データ挿入処理が行われた、連続するデータブロックに対して上記暗号化処理が行なわれることを特徴とする請求項 8 に記載のデータ送出方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、主データ及び付加データを暗号化して送 out するデータ送出装置、データ送出方法に関するものである。

【0002】

【従来の技術】

例えば著作権保護が必要なデータ、秘密性の高いデータ、プライバシーにかかる私的データなど、外部に漏洩することが好ましくないデータの伝送に際しては

、暗号化処理が行われることが多い。

例えば図 1 1 に或る送信装置 1 0 1 から受信装置 1 0 2 に対してデータを暗号化して伝送するモデルを示す。

#### 【 0 0 0 3 】

いま、伝送しようとするデータが送信装置 1 0 1 に入力されたとすると、送信装置 1 0 1 は、まず暗号化部 1 1 1 で暗号化処理を施し、暗号化されたデータ D T s を生成する。

そしてそのデータ D T s は送信部 1 1 2 から送信出力される。

送信出力されたデータ D T s は例えば I E E E 1 3 9 4 バスなどの伝送路 1 0 3 により、受信装置 1 0 2 に送られることになる。

受信装置 1 0 2 では、伝送路 1 0 3 から送信されてきたデータ D T s を受信部 1 2 1 で受信し、復号部 1 2 2 で暗号解読処理を行うことで、元のデータを得ることができる。

#### 【 0 0 0 4 】

##### 【発明が解決しようとする課題】

このように伝送路 1 0 3 においては暗号化されたデータ D T s が送信されることで、仮に伝送路 1 0 3 においてデータ D T s が取り出されたとしても、伝送データの内容は秘密性が保たれるものとなる。

しかしながら、例えば著作権保護を目的として音楽データ等を図 1 1 のようなシステムで伝送する場合、暗号を解読され、結果として違法なコピーが行われるおそれがある。

#### 【 0 0 0 5 】

ここで、図 1 1 に破線で示すように、何らかの手段で伝送路 1 0 3 から暗号化されたデータ D T s が取り出されたとする。

通常は、データ D T s を解析しても、元のデータ自体の内容がわからないため、暗号の解読は困難である。

ところが、元のデータの内容が明白にわかる部分としての暗号化データ D T s を抽出されると、その元のデータ内容と暗号化データを比較解析することで暗号化アルゴリズムが知られてしまう危険性がある。

そして暗号化アルゴリズムが解読されれば、悪意のユーザーによればその後データの違法な取り込みが容易に可能となってしまう。つまり著作権侵害となるような行為を実行可能としてしまう。

## 【0006】

元のデータの内容が明白なものとしては、例えば音楽データ等と同時に伝送される付加データ内の一部が考えられる。

一般に、音楽データ、映像データ等のデジタルデータコンテンツの伝送を行う場合、音楽や映像としての主データだけでなく、各種の付加データが付加されることが行われている。

例えば音楽データでいえば、曲名、歌詞、作詞作曲者名、アーティスト名などのテキストデータや、イメージ画像、写真画像などの画像データが、付加データとして同時に伝送される。

## 【0007】

これらの付加データとしては、伝送前の段階で光ディスク、ハードディスク、メモリカードなどのメディア上に、音楽データとともに既に記録されているものや、伝送時に新たに付加するものなどがある。

そして曲名、歌詞などの付加データであっても、メディア上において既に暗号化されて記録されている場合は、その付加データは上記の暗号化データDTsに対して「元の内容が明白なデータ」とはならない。つまり伝送の際の暗号化部111での暗号化の前の段階で既に暗号化されたデータであるためである。

## 【0008】

例えば伝送路103から暗号化データDTsを抽出した悪意のユーザが、伝送されている音楽の曲名を知り、暗号化データDTsのうちのその曲名データ部分を抽出して比較解析したとしても、暗号化される前の曲名データが既に暗号化されていれば、暗号化部111での暗号化アルゴリズムの解析はほぼ不可能となる。

## 【0009】

また、画像データの場合は、画像フォーマット、圧縮方式などのデータ形式の多様性から、画像自体がわかっているとしても、その画像データ自体は通常わからない

。従って悪意のユーザーが画像データ部分を元にして暗号化アルゴリズムを解くことも不可能に近い。

【 0 0 1 0 】

ところが、暗号化部 1 1 1 での処理の前で暗号化されていない付加データがあった場合、その付加データの元のデータ内容を悪意のユーザーが予測できるものがある。

例えば音楽データの場合、伝送時に I S R C (International Standard Recording Code) を付加することが行われる。

この I S R C は音源 (楽曲) に固有に付される国際規格コードであり、各音源に対して国名、会社名、録音年、レコーディング番号などを示すコードとされる。

そして或る楽曲についての I S R C は、例えば C D 等の販売に用いられる音楽カタログなどから知ることができる。

従って、伝送データに I S R C が付加データとして付加されていた場合、悪意のユーザーにとっては、それは「元の内容が明白なデータ」となり、その暗号化データ D T s から I S R C が付加された部分を抽出し、実際の I S R C のデータと比較解析することで、暗号化アルゴリズムが解析できる可能性が生ずる。

【 0 0 1 1 】

また I S R C に限らず、例えば曲名、アーティスト名、ディスク製造番号などであっても、暗号化部 1 1 1 での処理前に既に暗号化が施されているのであれば、それらも悪意のユーザーにとって「元の内容が明白なデータ」となり、暗号化アルゴリズムの解析や、著作権侵害行為を可能とってしまう可能性がある。

【 0 0 1 2 】

従って、音楽データ等の著作権保護が必要なデータについて、機器間の伝送、記録媒体への記録のための伝送、或いは公衆回線等を用いた音楽配信システムにおける伝送などの広範囲の分野で、上記の危険性が内包されており、このため元の内容が明白なデータを伝送する場合でも、違法な暗号解読を防止できるような技術が求められている。



## 【 0 0 1 3 】

## 【課題を解決するための手段】

本発明はこのような状況に鑑みて、伝送されるデータについて、容易に暗号解読ができないようにする技術を提供するものである。

## 【 0 0 1 4 】

このため本発明では、主データと付加データとが配される複数のデータブロックを連続的に送出することで、一連の主データ及び上記一連の主データに係る付加データを送出するデータ送出装置において、上記付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入する付加データ挿入手段と、上記付加データ挿入手段での付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行う暗号化手段と、上記暗号化手段により暗号化された連続するデータブロックを送出する送出手段とを備えるようにする。

例えば上記付加データ挿入手段は、暗号化されていない付加データを、ランダムに選択したデータブロックに挿入する。

或いは上記付加データ挿入手段は、暗号化されていない付加データ、及び暗号化されている付加データを、ランダムに選択したデータブロックに挿入する。

## 【 0 0 1 5 】

また、上記データブロックの一部に乱数データを挿入する乱数データ挿入手段をさらに備え、上記暗号化手段は、上記付加データ挿入手段での付加データ挿入処理、及び上記乱数データ挿入手段での乱数データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行うようにする。

また上記乱数データ挿入手段は、データブロック内における無効データ部分に、上記乱数データを挿入する。

## 【 0 0 1 6 】

またデータ送出装置は、それぞれ異なる機器としての送信装置、受信装置においてデータ伝送を行う場合の、上記送信装置として実現する。或いは、記録媒体に記録を行う記録装置における記録データの送出装置として実現されるようにする。

## 【 0 0 1 7 】

また本発明のデータ送出方法は、付加データを、一連の主データを構成する上記連続したデータブロックのうちでランダムに選択したデータブロックに挿入し、付加データ挿入処理が行われた、連続するデータブロックに対して暗号化処理を行ない、暗号化された連続するデータブロックを送出する。

また、上記データブロックの一部に乱数データを挿入する乱数データ挿入処理が行われるようにし、上記付加データ挿入処理、及び上記乱数データ挿入処理が行われた、連続するデータブロックに対して上記暗号化処理が行なわれるようにする。

## 【 0 0 1 8 】

即ち本発明では、送信の際の暗号化を行う前における連続したデータブロックに対して、付加データをランダムに選択したデータブロックに付加することで、付加データが付加される位置が連続するデータブロック内でランダムなものとなるようにする。つまり伝送されている暗号化データにおいて、「元の内容が明白なデータ」が配されている位置がわからないようにすることで、「元の内容が明白なデータ」に相当する暗号化データを抽出できないようにし、これによって暗号アルゴリズムが解読できないようにする。

またデータブロックの一部に乱数データを挿入することで、より暗号アルゴリズムの解読を困難とする。

## 【 0 0 1 9 】

## 【発明の実施の形態】

以下、本発明の実施の形態を次の順に説明する。

1. 送信装置に本発明を採用する例
2. IEEE 1394 の伝送フォーマット
3. IEEE 1394 でオーディオパケットデータを伝送する場合の付加データのランダム挿入例
4. 記録装置に本発明を採用する例

## 【 0 0 2 0 】

## 1. 送信装置に本発明を採用する例

本発明のデータ送出装置（データ送出方法）を、送信装置に採用する実施の形態を説明する。

図 1 は、或る 2 つの機器が例えば I E E E 1 3 9 4 バスによる伝送路 3 により接続されている場合に、送信装置 1 を有する機器から受信装置 2 を有する機器に音楽データ等のデータ D T、及びデータ D T に付随する付加データ D a 1、D a 2 を伝送するモデルにおいて本発明の実施の形態を示したものである。

パケット構造については後述するが、データ D T は、例えば 1 ビットデジタルオーディオデータを、所定の伝送プロトコルに合致するフォーマットに基づいてパケット化（ブロック化）したものであるとする。また付加データ D a 1、D a 2 は、そのブロック内に含まれて伝送される。

## 【 0 0 2 1 】

1 ビットデジタルオーディオデータとは、通常の C D（Compact Disc）におけるオーディオデータよりも高品位なデータとして開発されたものであり、サンプリング周波数を例えば C D 方式における 4 4 . 1 K H z の 1 6 倍という非常に高いサンプリング周波数である 2 . 8 4 2 M H z として  $\Delta \Sigma$  変調された 1 ビットデータのことであり、周波数帯域は D C 成分 ~ 1 0 0 K H z の広範囲とされ、ダイナミックレンジはオーディオ帯域全体で 1 2 0（d B）を実現できるデータ形式である。

なお、本例ではこのような 1 ビットデジタルオーディオデータをパケット化して伝送する場合を例に挙げるが、もちろん伝送されるデータ自体の形式、種別はどのようなものでもよい。

## 【 0 0 2 2 】

図示するように送信装置 1 は、ブロック処理部 1 0、ランダムデータ付加部 1 1、暗号化部 1 2、送信部 1 3 が設けられる。

この送信装置 1 に対しては、伝送するデータとして、例えば光ディスク、ハー

ドディスク、メモ리카ード等の所要のメディアから読み出された1ビットデジタルオーディオデータとしてのデータDT、及びこの主たるデータDTに付随して、同じくメディアから同時に読み出された付加データDa1が供給される。なお、この場合においてデータDa1はメディア上で既に暗号化されて記録されていたものとし、送信装置1に入力される時点では暗号化された付加データとなっているものとする。

また、当該1ビットデジタルオーディオデータとしてのデータDTの伝送に際して、さらに付加データDa2が伝送されるべきデータとして与えられるものとする。具体例としては付加データDa2はISRCであるとする。そして、このISRCは送信装置1に入力される時点では暗号化されていないデータである。

#### 【0023】

ブロック処理部10は、データDT、付加データDa1、Da2について、後述するIEEE1394による伝送フォーマットに即したブロックとしてのデータストリームに形成する処理を行う。

具体的なブロック例は後述するが、所定のチャンネル数の1ビットデジタルオーディオデータを配したブロックが連続されることで、例えば1つの楽曲としてのデータストリームが形成される。また各ブロックには付加データDa1、Da2を配する領域や無効データが充填される領域が設定されている。

ここで、本例では少なくとも付加データDa2について、或いは付加データDa1、Da2について、連続するブロックのうちでランダムに選択したブロック内に配置されるようにするものである。

#### 【0024】

ランダムデータ付加部11は内部に乱数発生回路を備え、送信しようとするデータDT（パケットデータを構成するブロック）の所要の部分に乱数発生回路で発生させた乱数データを付加する動作を行う。

暗号化部12は、ランダムデータ付加部11の出力に対して所定の暗号アルゴリズムでの暗号化処理を施す。

送信部13は暗号化部12の出力をIEEE1394バスによる伝送路3に送出する動作を行う。

【 0 0 2 5 】

受信装置 2 は、受信部 2 1、復号部 2 2、ブロックデコード部 2 3 を備える。

受信部 2 1 は、伝送路 3 から供給されるデータを受信して取り込む動作を行う。

復号部 2 2 は、上記暗号化部 1 2 での暗号化アルゴリズムに対応して暗号解読処理を行う部位である。

ブロックデコード部 2 3 は、上記ランダムデータ付加部 1 1 で付加された乱数データ部分を除去するとともに、一連のブロックデータから付加データ D a 1、D a 2 を抽出する。もちろん各ブロックデータから 1 ビットデジタルオーディオデータとしてのデータ D T も取り出す。

【 0 0 2 6 】

このような送信装置 1、受信装置 2 においてデータ D T の伝送は次のように行われる。

パケットデータとして伝送しようとするデータ D T、付加データ D a 1、D a 2 が送信装置 1 に入力されたとなると、送信装置 1 は、まずブロック処理部 1 0 でパケットを構成する一連のブロックデータによるデータストリームを生成する。このとき上記のように付加データ D a 2（又は D a 1、D a 2）はランダムなブロックに挿入する。

ランダムデータ付加部 1 1 で、パケット内の所定の部位に乱数データを挿入する。具体例は後述するが、パケットデータ内の無効データ部分に乱数データを挿入することになる。

ランダムデータ付加部 1 1 で乱数データが挿入されたデータ D T a d は、続いて暗号化部 1 2 に供給され、暗号化処理が施される。

暗号化されたデータ D T s は、送信部 1 3 に供給され、送信部 1 3 から伝送路 3 に対して送出されることになる。

【 0 0 2 7 】

このように送信されたデータ D T s を受信する受信装置 2 では、まず伝送路 3 から供給されてきたデータ D T s を受信部 2 1 で受信し、復号部 2 2 に供給する。復号部ではデータ D T s に対する暗号解読処理を行うことで、暗号化前のデー

タ、即ち乱数データが付加されている状態のデータDTadが出力される。

このデータDTadはブロックデコード部23に供給され、ランダムデータ部分が除去されるとともに、データDT、付加データDa1、Da2が抽出される。つまり当初の送信データが得られることとなる。

#### 【0028】

ここで破線で示すように、何らかの手段で伝送路3から暗号化されたデータDTsが取り出された場合を考える。

上述したようにデータDTsにおいて元の内容が明白な部分（例えば付加データDa2となるISRC）が抽出されると暗号化アルゴリズムが解読されるおそれがある。

しかしながら本例の場合、付加データDa2は、一連のブロックシーケンスのうちでどのブロックに挿入されるかは、全くランダムなものとなっている。従って實際上、伝送路3から暗号化データDTsを抽出しようとする悪意のユーザーにとって、付加データDa2に相当する部分としての暗号化データDTsを抽出することは不可能となる。つまり「元の内容が明白なデータ」の部分の暗号化データDTsは抽出できない。従って暗号解読は困難となる。

#### 【0029】

また、仮にデータDTsにおいて、付加データDa2の部分が抽出されたとしても、データDTsは、乱数データを含めた上で暗号化されているため、データDTsの解析処理において、データDTs上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することは一層困難となる。

#### 【0030】

以上のことから、本例によれば伝送路3で伝送されるデータについて暗号解読はほぼ不可能となり、従って、著作権保護を要するデータの伝送などに非常に好適なものとなる。

また送信装置1側では、ブロック処理部10で付加データDa2の挿入ブロックをランダム化するという処理、及びランダムデータ付加部11で乱数データを挿入するという処理を加えるだけでよく、送信装置1としての構成がさほど複雑

化することもない。従って各種の機器への導入は容易なものとなる。

#### 【0031】

なお付加データDa2の挿入ブロックをランダム化しても、受信装置2側ではデコードが困難になることはない。詳しくは後述するが、付加データDa2を明示するラベルがブロック内に配されていることで、受信装置2のブロックデコード部23は、そのラベルに応じて付加データを抽出すればよいためである。また乱数データの除去も同じ理由で容易である。つまりブロック内の無効データ部分に乱数データを挿入するため、ブロックデコード部23はラベルによって無効データ部分とされている部分を捨て去ればよいのみとなる。

従って受信装置2としての構成も複雑化することもなく、各種の機器への導入は容易である。

#### 【0032】

### 2. IEEE1394の伝送フォーマット

ここでIEEE1394による伝送フォーマットについて説明する。

IEEE1394方式でのデータ伝送では、例えば図2(a)に示すように、所定の通信サイクル（例えば $125\mu\text{sec}$ ）毎に時分割多重によって行われる。そして、この信号の伝送は、サイクルマスタと呼ばれる機器（IEEE1394バス上の任意の1台の機器）が通信サイクルの開始時であることを示すサイクルスタートパケットCSPをバス上へ送出することにより開始される。なお、サイクルマスタは、バスを構成するケーブルに各機器を接続したとき等に、IEEE1394で規定する手順により自動的に決定される。

#### 【0033】

1通信サイクル中における通信の形態は、ビデオデータやオーディオデータなどのリアルタイム性を必要とするデータを伝送するアイソクロナス伝送（Iso）と、制御コマンドや補助的なデータなどを確実に伝送するアシンクロナス伝送（Asy）の2種類の伝送が行われる。

各通信サイクル中では、アイソクロナス伝送用のアイソクロナスパケット I s o が、アシンクロナス伝送用のアシンクロナスパケット A s y より先に伝送される。

アイソクロナスパケット I s o の通信が終了した後、次のサイクルスタートパケット C S P までの期間が、アシンクロナスパケット A s y の伝送に使用される。従って、アシンクロナスパケット A s y が伝送できる期間は、そのときのアイソクロナスパケット I s o の伝送チャンネル数により変化する。また、アイソクロナスパケット I s o は、1 通信サイクル毎に予約した帯域（チャンネル数）が確保される伝送方式であるが、受信側からの確認は行わない。

アシンクロナスパケット A s y で伝送する場合には、受信側からアクノリッジメント（A c k）のデータを返送させて、伝送状態を確認しながら確実に伝送させる。

#### 【 0 0 3 4 】

図 2（b）に、C I P (Common Isochronous Packet) の構造を示す。つまり、図 2（a）に示したアイソクロナスパケット I s o のデータ構造である。

例えば、上述した 1 ビットデジタルオーディオデータは、I E E E 1 3 9 4 通信においては、アイソクロナス通信によりデータの送受信が行われる。つまり、リアルタイム性が維持されるだけのデータ量をこのアイソクロナスパケットに格納して、1 アイソクロナスサイクル毎に順次送信するものである。

#### 【 0 0 3 5 】

アイソクロナスパケットは、図 2（b）のように、1 3 9 4 パケットヘッダ、ヘッダ C R C、C I P ヘッダ、データ部、データ C R C から成る。

この C I P 構造として、例えば 2 チャンネルの 1 ビットデジタルオーディオデータの伝送に用いる場合における具体例を図 3 に示している。

#### 【 0 0 3 6 】

図 3 では、横方向に 3 2 ビット（4 バイト）を示しているが、その 1 行分のデータ、つまり 3 2 ビットが 1 カドレット（quadlet）と呼ばれる。

C I P の先頭 3 2 ビット（1 カドレット）は、1 3 9 4 パケットヘッダとされている。



1394 パケットヘッダにおいては、16ビットのデータレングス (data \_Length)、2ビットのタグ (tag)、6ビットのチャンネル (channel)、4ビットのタイムコード (t code)、4ビットのシンク (sy) が配される。

そして、1394 パケットヘッダに続く1カドレットの領域はヘッダCRCが格納される。

#### 【0037】

ヘッダCRCに続く2カドレットの領域がCIPヘッダとなる。

CIPヘッダの上位カドレットの先頭2バイトには、それぞれ‘0’ ‘0’ が格納され、続く6ビットの領域はSID (送信ノード番号) を示す。SIDに続く8ビットの領域はDBS (データブロックサイズ) であり、データブロックのサイズ (パケット化の単位データ量) が示される。続いては、FN (2ビット)、QPC (3ビット) の領域が設定されており、FNにはパケット化する際に分割した数が示され、QPCには分割するために追加したカドレット数が示される。

SP (1ビット) にはソースパケットのヘッダのフラグが示され、DBCにはパケットの欠落を検出するカウンタの値が格納される。

なお、図中「rsv」はリザーブ、つまり未定義の領域を示している。

#### 【0038】

CIPヘッダの下位カドレットの先頭2バイトにはそれぞれ‘1’ ‘0’ が格納される。そして、これに続いてFMT (6ビット)、FDF (8ビット)、SYT (16ビット) の領域が設けられる。

FMTには信号フォーマット (伝送フォーマット) が示され、ここに示される値によって、当該CIPに格納されるデータ種類 (データフォーマット) が識別可能となる。具体的には、MPEGストリームデータ、Audioストリームデータ、デジタルビデオカメラ (DV) ストリームデータ等の識別が可能になる。

FDFは、フォーマット依存フィールドであり、上記FMTにより分類されたデータフォーマットについて更に細分化した分類を示す領域とされる。オーディオに関するデータであれば、例えばリニアオーディオデータであるのか、MID

I データであるのかといった識別が可能になる。

例えば 1 ビットデジタルオーディオデータであれば、先ず FMT により Audio ストリームデータの範疇にあるデータであることが示され、FDF に規定に従った特定の値が格納されることで、その Audio ストリームデータは 1 ビットデジタルオーディオデータであることが示される。

SYT は、フレーム同期用のタイムスタンプが示される。

#### 【 0 0 3 9 】

このような CIP ヘッダに続けては、FMT、FDF によって示されるデータが、データ部としての  $n$  個のデータブロック（ブロック # 0 ~ #  $n$ ）のシーケンスによって格納される。FMT、FDF により 1 ビットデジタルオーディオデータであることが示される場合には、このデータブロックとしての領域に 1 ビットデジタルオーディオデータが格納される。

そして、データブロックに続いて最後にデータ CRC が配置される。

#### 【 0 0 4 0 】

この図 3 では、データ部に 2 チャンネルの 1 ビットデジタルオーディオデータが配されている例を示している。これは、IEEE 1394 バスによるデータ伝送について適用できる AM 824 と呼ばれる伝送プロトコルに基づいた例であり、その場合において 1 ビットデジタルオーディオデータとして 2 チャンネルのオーディオデータを伝送する場合のパケット構造例である。

#### 【 0 0 4 1 】

上述のように 32 ビット（4 バイト）を 1 カドレット（Quadlet）と呼ぶとすると、2 チャンネルデータの場合、4 カドレット（ $q_1 \sim q_4$ ）で 1 つのブロックが形成され、このブロックが連続するものとなる。

#### 【 0 0 4 2 】

各カドレットにおける先頭のバイト（バイト 0）は、ラベルとされている。ラベルとは、そのカドレットに配されるデータの識別情報となる。

ラベルとしての値及び意味を図 4 に示す。

図示するようにラベル値に対して各種の意味が定義されており、例えばラベル値 40h ~ 4Fh は、DVD（Digital Versatile Disc）システムで採用されて

いるマルチビットリニアオーディオデータに対応するものとされる。なお、「h」を付した数値は16進表記のものである。

またラベル値50h～57hは、1ビットデジタルオーディオデータに対応する値、ラベル値58h～5Fhは、エンコードされた1ビットデジタルオーディオデータに対応する値、ラベル値80h～83hはMIDIデータに対応する値とされる。

さらにC0h～EFhはアンシラリデータ (Ancillary Data; 補助データ) を意味するなど、ラベル値は識別情報として機能するために各種定義されている。

#### 【0043】

各ラベル値についての詳細な定義の説明は本発明と直接関係がないため説明を省略するが、図3に示した値についてのみ述べると次のようになる。

#### 【0044】

図3においてブロック#0の第1カドレットq1をみると、ラベル値は「D1h」とされている。従って第1カドレットq1はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「00h」とされている。

このときバイト2、バイト3が実際の補助データ内容となるが、ここではバリディティフラグ (Validity Flag) V、コピーコントロール情報 (Track Attribute)、チャンネル数 (Ch Bit Num)、スピーカ配置情報 (Loudspeaker Config) が記述される。

#### 【0045】

第2カドレットq2ではラベル値は「50h」とされる。ラベル値50h～57hは、1ビットデジタルオーディオデータに対応する値であるが、「50h」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第3カドレットq3ではラベル値は「51h」とされる。「51h」は、マルチチャンネルのデータを配したブロックの2番目以降のデータであることを示す。

従って、第2、第3カドレット (q2、q3) では、チャンネル1 (例えばL

チャンネル)、チャンネル2(例えばRチャンネル)の2チャンネルの1ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト1～バイト3の3バイトで記述される。

#### 【0046】

第4カドレットq4では、ラベル値は「CFh」とされている。これはアンシラリデータの範疇であるが、「CFh」は特に無効データ(NO DATA)を示す値として定義されている。またバイト1はサブラベルとして無効データの内容を示す値とされており、この例では「CFh」とされている。

そしてこのときバイト2、バイト3が無効データにより充填される。

なお、第4カドレットq4として無効データが配されるカドレットが形成されるのは、1つのブロックは偶数個のカドレットで形成されるべく規定されているためである。

#### 【0047】

ブロック#1の第1カドレットq1では、ラベル値は「D1h」とされている。従って第1カドレットq1はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト1はサブラベルとされて「01h」とされている。

このときはバイト2、バイト3の補助データ内容は、サブリメンタリデータとされる。

第2～第4カドレットはブロック#0と同様である。

#### 【0048】

このように各ブロックが構成されて、アイソクロナスパケットIsoにおけるデータ部が形成される。

なお、ここで示したアンシラリデータ、サブリメンタリデータは、図1に示した付加データDa1に相当するデータとなる。従ってこれらは、例えば1ビットデジタルオーディオデータとともにメディア上に記録されていた付加データであって、その段階で既に暗号化された内容のデータであるとする。

付加データDa2となる例えばISRCについては図3では示していないが、続いて図5以降で説明するように、例えばラベルが「C0h」、サブラベルが「

0 1 h」以降の値として設定されたカドレットに配されることとなる。なお、このラベルの値は一例にすぎない。

#### 【 0 0 4 9 】

### 3. I E E E 1 3 9 4 でオーディオパケットデータを伝送する場合の付加データのランダム挿入例

以上のような I E E E 1 3 9 4 による伝送フォーマットを用いて、図 1 で説明したようにデータを伝送する場合の具体例を以下、説明していく。即ち I E E E 1 3 9 4 の伝送路 3 でオーディオパケットデータを伝送する場合のブロックシーケンスの例である。

#### 【 0 0 5 0 】

まず図 5 でブロックシーケンスの概要を述べる。

上記図 3 で示したデータ部を構成するブロック # 0、# 1・・・に配されるオーディオデータは、元々の 1 ビットデジタルオーディオデータとしてのトラック（楽曲単位）から見ると図 5 に示す関係となる。

図 5（a）は 1 つの楽曲としてのデータ群となるトラック（プログラム）をトラック # N として示しているが、このトラック # N は図 5（b）のように複数のフレームから構成される。

公知のように 1 つのフレームは 7 5 H z 周期、即ち 1 3. 3 m s e c 分のオーディオデータに相当する単位である。

そして図 5（c）のように 1 フレームは 1 5 6 8 ブロック（ブロック # 0 ~ # 1 5 6 7）で構成される。

なお、図 5 にフレームとして示すブロック # 0 ~ # 1 5 6 7 の部分は、図 2、図 3 で説明したアイソクロナスパケット I s o 内のデータ部に相当する部分である。

#### 【 0 0 5 1 】

図 5（d）は、ブロック # 0 ~ # 1 5 6 7 の内容の例を示したものである。 2

チャンネルの1ビットデジタルオーディオデータの伝送を考えた場合、上記図3で説明したように各ブロックは4カドレット ( $q_1 \sim q_4$ ) で形成され、カドレット  $q_2$ ,  $q_3$  にオーディオデータが配される。

そして上述のようにカドレット  $q_4$  はラベルが「CFh」とされて、無効データが配される部分となる。

#### 【0052】

また図3で説明したように第1カドレット  $q_1$  はアンシラリデータ Anc i、サブリメンタリデータ Suppl i が配されるが、フレームを構成する先頭のブロック#0は、ラベル、サブラベルが「D1h」「00h」とされて、図3に示したようにアンシラリデータ Anc i (付加データ Da 1) が配される。

またブロック#1以降は、カドレット  $q_1$  は、ラベル、サブラベルが「D1h」「01h」とされて、サブリメンタリデータ Suppl i (付加データ Da 1) が配される。

なお、先頭ブロック#0にアンシラリデータ Anc i が配されることはAM824の伝送フォーマット上、規定されているが、ブロック#1～#1567においては、カドレット  $q_1$  にどのようなデータを配しなければならないかは規定されていない。ただし通常はブロック#1から所定数のブロックに連続して、サブリメンタリデータ Suppl i が配されることになる。

#### 【0053】

また或るブロック#yのカドレット  $q_1$  は、ラベルが「C0h」とされて、ISRC等の付加データ Da 2 が配される。

また、これら付加データ Da 1、Da 2 を配する必要がなくなったブロックとして、この場合ブロック#z、#1567を例に挙げているが、それらのブロックはラベル、サブラベルが「CFh」「D1h」とされて、無効データが配される。

#### 【0054】

このようなブロック#0～#1567が、伝送するデータの1フレームに相当する、一連の連続したブロックシーケンスとなるが、まずこの図5(d)を用いて、本例のブロック処理部10で設定されるブロックシーケンスの説明の前に、

ランダムデータ付加部 1 1 での乱数データの挿入方式を説明する。

【 0 0 5 5 】

図 5 ( d ) のようなブロックシーケンスに対して、送信装置 1 のランダムデータ付加部 1 1 では、無効データの部分に乱数データを挿入すればよい。即ち各ブロックにおいて斜線部を付した無効データ部分に乱数データを挿入する。

具体的にはランダムデータ付加部 1 1 では 1 パケットあたりに 2 バイトの乱数データを生成し、無効データのカードレット、つまりラベル値 = 「 C F h 」 のカードレットのバイト 2, 3 の 2 バイトに挿入するものである。

【 0 0 5 6 】

このように乱数データを挿入することにより、パケット内のオーディオデータが仮にオールゼロ、あるいは「 9 6 h 」などの固定パターンであったり、 I S R C 等の付加データ D a 2 として、暗号化部 1 2 での暗号化前の元のデータ内容が明白な部分があったとしても、そのデータと乱数データが混在した状態で暗号化されることになるため、元のデータ内容が見えないものとなる。つまり上述のように暗号解読を困難にできる。

なお、暗号化部 1 2 で暗号化処理を行うデータ単位がブロック単位より小さい単位、例えば 8 バイト ( 2 カドレット ) 単位であった場合は、その 8 バイト毎に、一部に乱数データが挿入されるようにすることが好ましい。

【 0 0 5 7 】

本例の送信装置のブロック処理部 1 0 では、一連のブロック # 0 ~ # 1 5 6 7 の中で、付加データ D a 2 を挿入するブロックをランダムに選択するものである。

この処理を図 6, 図 7 で説明する。

図 6、図 7 は、図 5 ( d ) に示した 1 フレーム内のブロックシーケンスを、各ブロックの第 1 カドレット q 1 のみで示している。

【 0 0 5 8 】

なお、図 6 ( a ) として、比較のために通常のブロックシーケンスを示す。

図 6 ( a ) の通常のブロックシーケンスの場合は、先頭ブロック # 0 にアンシラリデータ A n c i が配され、続いてブロック # 1 ~ # ( x - 1 ) まで連続して

サブメンタリデータ *Suppli* が配される。つまり先頭ブロックから順に付加データ *Da1* が配されていく。

もし *ISRC* 等の付加データ *Da2* を挿入することが不要な場合は、ブロック # (x) ~ # 1567 については、カドレット *q1* は無効データ部分とされるが、付加データ *Da2* を挿入する場合は、サブメンタリデータ *Suppli* に続いて、ブロック # (x) 以降に順に付加データ *Da2* (*ISRC* 等) が挿入される。図6 (a) の例の場合は、ブロック # (x) ~ ブロック # (x+2) は、それぞれラベルが「C0h」で、サブラベルが順に「00h」「01h」「02h」とされて、それぞれ *ISRC* としての情報が挿入されている。

そしてブロック # (x+3) ~ ブロック # 1567 までは無効データ (斜線部) が充填される。なお、上述のようにこの無効データ部分には乱数データが挿入されることになる。

#### 【0059】

しかしながらこのような通常のブロックシーケンスによれば、*ISRC* が挿入された位置 (ブロックのナンバ) が悪意のユーザーにとって予測し得るものとなるおそれがある。つまり付加データ *Da1* の挿入に用いられるブロック数が固定的であるとする、その次のブロック # x が *ISRC* が挿入されたブロックであるとわかってしまう。すると、暗号化データ *DTs* のうちでブロック # x の部分を抽出するとともに、何らかの手段で伝送されている楽曲についての *ISRC* を知ると、暗号化アルゴリズムが解析しやすくなってしまう。

#### 【0060】

そこで本例のブロック処理部 10 では上述のように、少なくとも付加データ *Da2* については、ランダムにブロックを選択して挿入するようにする。

図6 (b) が付加データ *Da2* をランダムに挿入する場合のブロックシーケンスの例である。

図示するように先頭のブロック # 0 にアンシラリデータ *Anci* が配され、続いてブロック # 1 ~ # (x-1) まで連続してサブメンタリデータ *Suppli* が配されることは通常のブロックシーケンスと同様としている。



## 【0061】

ここで付加データDa2はブロック#(x)以降に挿入されるものとなるが、付加データDa2を挿入するブロックは、ブロック#(x)～#1567のうちでランダムに選択するようにする。

例えばこの図6(b)の場合は、付加データDa2としてのISRCが、ブロック#(x+1)、#(x+2)、#1567に挿入されている。

そしてこれら以外のブロックは無効データ(斜線部)が配される。これはランダムデータ付加部11で乱数データが配される領域となる。

## 【0062】

このようにブロック#(x)～#1567において付加データDa2がランダムに挿入されることは、各フレーム毎に行われる。

例えば図6(b)がフレーム#Mのブロックシーケンスであるとする、次のフレーム#(M+1)は、図7のようになる。例えばこの場合は、付加データDa2としてのISRCが、ブロック#(x)、#(x+3)、#1566に挿入されている。そしてこれら以外のブロックは無効データ(斜線部)が配される。

## 【0063】

即ち本例では、ブロック処理部10において、各フレームを構成するブロックシーケンス内で、付加データDa2についてはブロック#x～#1567内のランダムに選択したブロックに挿入するようにしている。

従って、各フレームを構成するデータストリーム内では、どのブロックに付加データDa2が挿入されているかは、全く予測できないものとなる。

そしてこのようなブロックシーケンスのデータが暗号化部12で暗号化データDTsとされて伝送路3に送出されるが、伝送路3から暗号化データDTsのうちで付加データDa2部分を抽出することはほぼ不可能となる。このため上述のように不正な暗号アルゴリズムの解析を防止できる。

また、上記のように無効データ部分に乱数データが挿入されることで、一層暗号アルゴリズムの解析を困難とすることができる。

## 【0064】

なお、以上のように付加データDa2がランダムなブロックに挿入されること

や、それによってフレーム毎に付加データ  $D a 2$  の位置が異なることとなっても受信装置 2 側では不都合はない。

つまり受信装置 2 のブロックデコード部 2 3 では、単に各フレームを構成するブロックから、ラベル = 「C 0 h」の部分を抽出すればよいためである。

#### 【0 0 6 5】

また、無効データ部分に乱数データを挿入することによっても、受信装置 2 側での処理が複雑とはならない。

即ち受信装置 2 のブロックデコード部 2 3 はラベル値 = 「C F h」のカドレットを捨てればよいのみであるためである。ラベル値 = 「C F h」のカドレットは無効データとして本来捨てられるものであるため、その意味でいえば、乱数データ除去のために何ら特別な処理を必要としないものともなる。

#### 【0 0 6 6】

ところで、ブロック処理部 1 0 でのブロックシーケンスの設定は、図 8 の例に示すように行ってもよい。

上記図 6 (b) 及び図 7 の例は、ブロック # (x) 以降で付加データ  $D a 2$  を挿入する位置をランダムに選択したが、図 8 の例はブロック # 1 ~ # 1 5 6 7 まをランダムに選択する対象とする例である。

#### 【0 0 6 7】

つまり、先頭のブロック # 0 についてはラベル、サブラベルが「D 1 h」「O 0 h」のアンシラリデータ  $A n c i$  を挿入するものと規定されているため、これを変えることはできないが、ブロック # 1 以降は任意である。そしてラベル、サブラベルでデータ内容が規定される限り、付加データ  $D a 1$  としてのサブリメンタリデータ  $S u p p l i$  や、付加データ  $D a 2$  としての  $I S R C$  は、どのブロックに挿入されていても、受信装置側では問題ない。

そこで、図 8 のようにサブリメンタリデータ  $S u p p l i$  を含めて、挿入するブロックをランダムに選択するようにしてもよい。

#### 【0 0 6 8】

図 8 の例の場合は、或るフレームにおいて付加データ  $D a 1$  としてのサブリメンタリデータ  $S u p p l i$  が、ブロック # 3、# 4、# (x + 2)、# 1 5 6 7

・・・に配されており、また付加データDa2としてのISRCが、ブロック#2、#4、#(x)・・・に配されている。

これらの付加データが挿入されなかったブロックは無効データが充填される（斜線部）。

もちろんこの図8は、或るフレームにおいてサプリメンタリデータSuppli及びISRCがランダムなブロックに挿入された場合の一例であり、次のフレーム、その次のフレームなどでは、サプリメンタリデータSuppliやISRCの順序は全く別の状態となる。

【0069】

このようにサプリメンタリデータSuppliまでも含めて、付加データDa1、Da2の挿入ブロックをランダムに選択することにより、例えばISRCなどの元の内容が明白なデータが挿入されている位置は、一段と予測できないものとなり、暗号解読の防止効果を強めることができる。

きな

【0070】

#### 4. 記録装置に本発明を採用する例

続いて、本発明のデータ送出装置（データ送出方法）を、所定のメディアにデータを記録する記録装置に採用する実施の形態を説明する。

【0071】

図9は所定の記録媒体（メディア）6に対してデータDT（及び付加データDa1、Da2）を記録できる記録装置である。

図示するように記録装置4は、入力されてくるデータDTに対する記録処理系として、暗号化部40、エンコード及び記録ドライブ部44、記録ヘッド（又はインターフェース）45が設けられる。

暗号化部40は、ブロック処理部46、ランダムデータ付加部41、暗号化部42、送出部43を有する。

## 【 0 0 7 2 】

このような記録装置 4 に対しては、上記の送信装置 1 の場合と同様に、例えば光ディスク、ハードディスク、メモ리카ード等の所要のメディア 6 に対して記録するデータとして、例えば 1 ビットデジタルオーディオデータなどのデータ DT、及びこの主たるデータ DT に付随する付加データ Da 1 が供給され、また例えば I SRC などの付加データ Da 2 が供給されるものとする。

## 【 0 0 7 3 】

ブロック処理部 4 6 は、データ DT、付加データ Da 1、Da 2 について、上述した IEEE 1 3 9 4 による伝送フォーマットに即したブロックとしてのデータストリームに形成する処理を行う。

そして少なくとも付加データ Da 2 については、或いは付加データ Da 1、Da 2 について、連続するブロックのうちでランダムに選択したブロック内に配置されるようにする。即ち図 6、図 7 或いは図 8 で説明したようにブロックシーケンスを設定する。

## 【 0 0 7 4 】

またランダムデータ付加部 4 1 は内部に乱数発生回路から発生させた乱数データを、ブロックの所要の部分、例えば無効データ部分に付加する。

ランダムデータ付加部 4 1 で乱数データが挿入されたデータ DT ad は、続いて暗号化部 4 2 に供給され、暗号化処理が施される。

暗号化されたデータ DT s は、送出部 4 3 に供給され、送出部 4 3 からエンコード及び記録ドライブ部 4 4 に送出される。

## 【 0 0 7 5 】

エンコード及び記録ドライブ部 4 4 は、供給されたデータ DT s に対して、記録を行うメディア 6 の記録フォーマット、変調方式に応じてエラー訂正符号の付加や各種エンコード処理を行い、記録ドライブ信号を生成する。

その記録ドライブ信号は記録ヘッド 4 5 に供給されて記録ヘッド 4 5 によりメディア 6 へのデータ書込が行われる。

例えばメディア 6 が光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどであれば、記録ドライブ信号に応じて光学ヘッド又は磁気ヘッドが駆動され

て記録が実行される。

また、メディア6がフラッシュメモリなどによるメモリカードのような形態であれば、インターフェース45によりメディア6に対して書込アクセスが行われることになる。

#### 【0076】

図10は所定の記録媒体（メディア）6からデータDTを再生できる再生装置である。

図示するように再生装置5は、メディア6からデータの読み出しを行う再生ヘッド（又はインターフェース）54、デコード部55、復号部50が設けられる。

復号部50は、取込部51、復号部52、ブロックデコード部53を備える。

#### 【0077】

この再生装置5では、例えばメディア6としての光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどから光学ヘッド又は磁気ヘッドとしての再生ヘッド54によって読み出されたデータ、或いはメディア6としてのメモリカードからインターフェース54を介した読出アクセスにより読み出されたデータは、デコード部55で、メディア6の記録フォーマットに応じたデコード処理やエラー訂正処理が行われる。そしてそのデコードされたデータは、即ち記録装置4で暗号化されたデータDTsであり、データDTsは取込部51により復号部50内に取り込まれ、復号部52で暗号解読処理される。

復号部52で、上記暗号化部42での暗号化アルゴリズムに対応した暗号解読処理を行うことで、ランダムデータが付加された状態のデータDTadとされる。そして、そのデータDTadがブロックデコード部53でランダムデータの除去処理が行われるとともに、付加データDa1、Da2の抽出、データDTの抽出が行われて、元のデータDTや付加データDa1、Da2が再生されるものとなる。

#### 【0078】

記録装置4が以上のように構成されることで、メディア6に記録されるデータにおいて、ISRC等の付加データDa2として元の内容が明白なデータは、ブ

ロックシーケンス上では位置が全く予測できないものとなる。

従ってメディア6に記録されたデータをデコードしても、付加データDa2に相当するデータ部分を抽出することは困難となり、この点で暗号解読は困難となる。

さらに乱数データが付加された後に暗号化されることで、暗号化前の段階で元のデータ内容が明白な部分がなくなる。

従ってメディア6から仮にI SRC等の付加データDa2に相当する部分が抽出されても、そのデータは、乱数データを含めた上で暗号化されているため、データDTsの解析処理において、データDTs上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することはほぼ不可能である。

#### 【0079】

つまりこのような記録装置によれば、メディア6に記録されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの記録などに非常に好適なものとなる。

また、上述した送信装置1の場合と同様に、記録装置4として構成がさほど複雑化することもなく、導入は容易である。

また、上述した受信装置2の場合と同様に、ランダムに挿入された付加データDa2の抽出や乱数データの除去は、ラベルに応じて実行すればよいので、再生装置5のブロックデコード部53の処理は簡易なものとなる。

#### 【0080】

なお、図9、図10として記録装置4、再生装置5を分けて示したが、これらの回路構成を1つの機器に設けて、記録再生装置とすることはもちろん可能である。

また、記録装置4（又は記録再生装置）としては、必ずしも暗号化部40を設けなくてもよい。例えば伝送路3を介して或る送信装置から伝送されてきたデータを記録する記録装置を考えると、その送信装置側が図1に示した構成を備えていれば、記録装置に伝送されてくるデータは、既にランダムな位置に付加データDa2が配されるとともに、乱数データが付加された上で暗号化されたデータD

T s となっている。従ってその場合、記録装置は暗号化部 4 0 は不要となる。そして再生装置は、図 1 0 に示した復号部 5 0 を備えることで、伝送され記録されたデータの再生を行うことができるようになる。

例えば音楽等の配信システムなどを想定すると、このような形態が好適なものとなる。

#### 【 0 0 8 1 】

以上、実施の形態を説明してきたが、本発明はさらに多様な構成例が考えられ、また送信装置、記録装置などの形態で多種多様な機器に導入できるものである。

また、上記例では送信装置 1 と受信装置 2 は有線としての I E E E 1 3 9 4 方式の伝送路 3 による伝送システムとしたが、他の伝送規格によるものでもよく、また衛星通信、無線電話通信、赤外線伝送などの無線伝送システムに本発明を適用できることはもちろんである。

また、伝送するデータは図 5 ～ 図 8 に示したようなブロックデータに限定されるものではなく、あらゆるデータの伝送に本発明を適用できる。

また上記例では、ブロックの無効データ部分に乱数データを挿入するようにしたが、このような処理を行わなくてもよい。例えば図 1, 図 9 のランダムデータ付加部 1 1, 4 1 は設けなくてもよい。即ちブロック処理部 1 0, 4 6 で付加データを挿入するブロックをランダムに選択する処理のみでも、十分に暗号解読を困難にする効果があるためである。

#### 【 0 0 8 2 】

また、付加データ D a 2 に相当する付加データは I S R C に限られず、予め暗号化されておらず、かつそのデータ内容がわかり得るものがあり、例えばディスクタイトル、アーティスト名、ディスク製造ナンバ等が、暗号化されないテキストデータなどでそのまま付加データとされる場合は、それらも上述の付加データ D a 2 に相当する。つまり、ランダムな位置に挿入されるべき付加データとなる。

## 【 0 0 8 3 】

## 【発明の効果】

以上の説明からわかるように、本発明によれば、伝送するデータとしての連続したデータブロックに対して、付加データをランダムに選択したデータブロックに付加することで、付加データが付加される位置が連続するデータブロック内でランダムなものとなるようにしている。これによって、伝送されている暗号化データにおいて、「元の内容が明白なデータ」が配されている位置がわからないようにし、「元の内容が明白なデータ」に相当する暗号化データを抽出できないようにしている。これによって暗号アルゴリズムの解読を困難にできるという効果がある。

従って本発明は著作権保護などを必要とするデータの伝送に非常に好適なものとなる。

## 【 0 0 8 4 】

またデータブロックの一部に乱数データを挿入することで、より暗号アルゴリズムの解読を困難とできる。

## 【 0 0 8 5 】

またデータ送出装置は、異なる機器としての受信装置に対してデータを伝送する送信装置とすることで、機器間のデータ伝送において上記効果を実現できる。

さらにデータ送出装置は、それぞれ記録媒体に記録を行う記録装置における記録データの送出装置とすることで、記録媒体に記録されているデータ、又は記録再生の過程のデータにおいて上記効果を実現できる。

## 【図面の簡単な説明】

## 【図 1】

本発明の実施の形態の送信装置及び受信装置のブロック図である。

## 【図 2】

IEEE 1394 による伝送フォーマットの説明図である。

## 【図 3】

IEEE 1394 のアイソクロナスパケットの説明図である。



【図 4】

実施の形態のパケットデータのラベルの説明図である。

【図 5】

実施の形態のブロックシーケンスの説明図である。

【図 6】

実施の形態の付加データのランダムな挿入例の説明図である。

【図 7】

実施の形態の付加データのランダムな挿入例の説明図である。

【図 8】

実施の形態の付加データについての他のランダムな挿入例の説明図である。

【図 9】

実施の形態の記録装置のブロック図である。

【図 1 0】

実施の形態の再生装置のブロック図である。

【図 1 1】

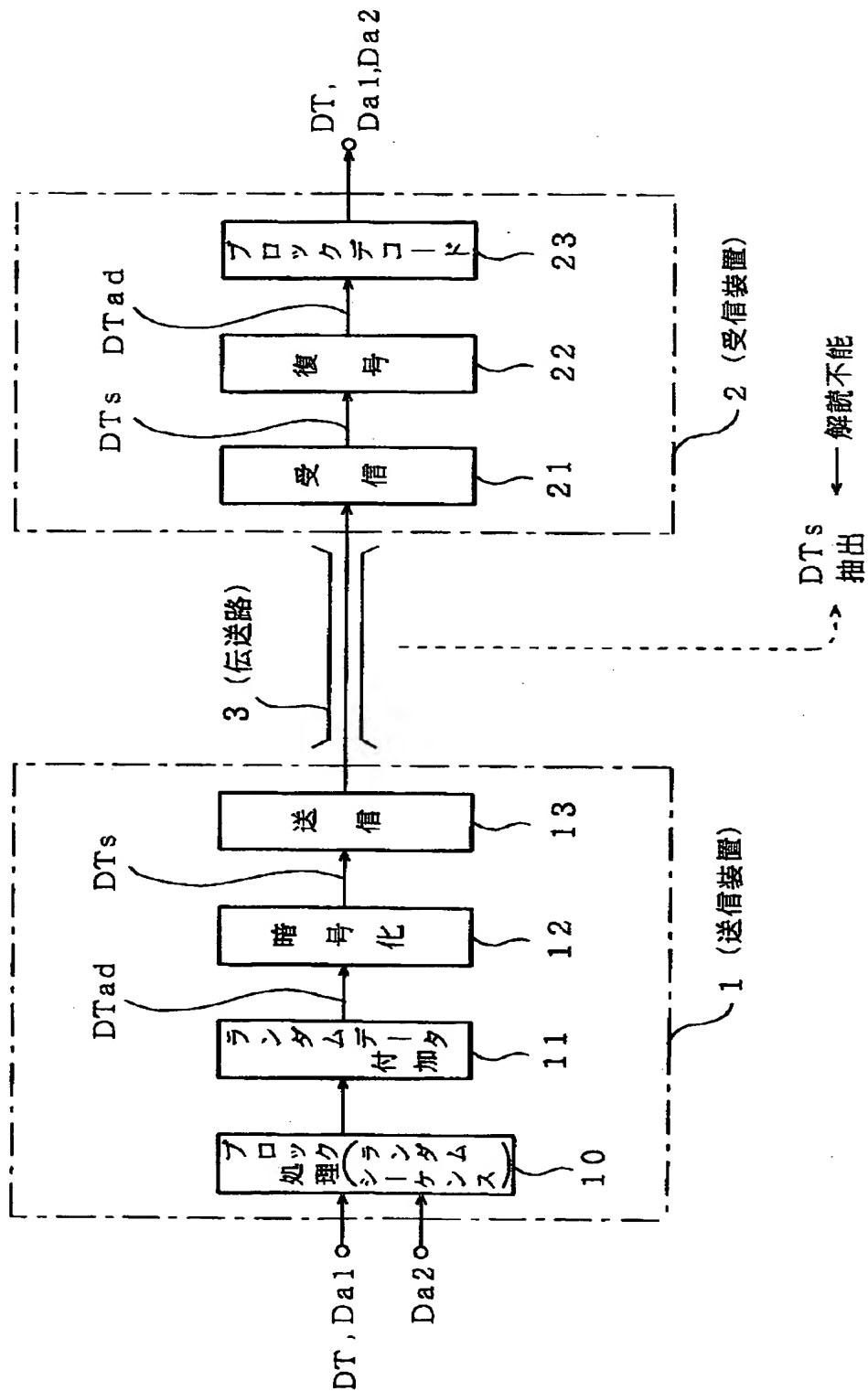
従来の伝送システムの説明図である。

【符号の説明】

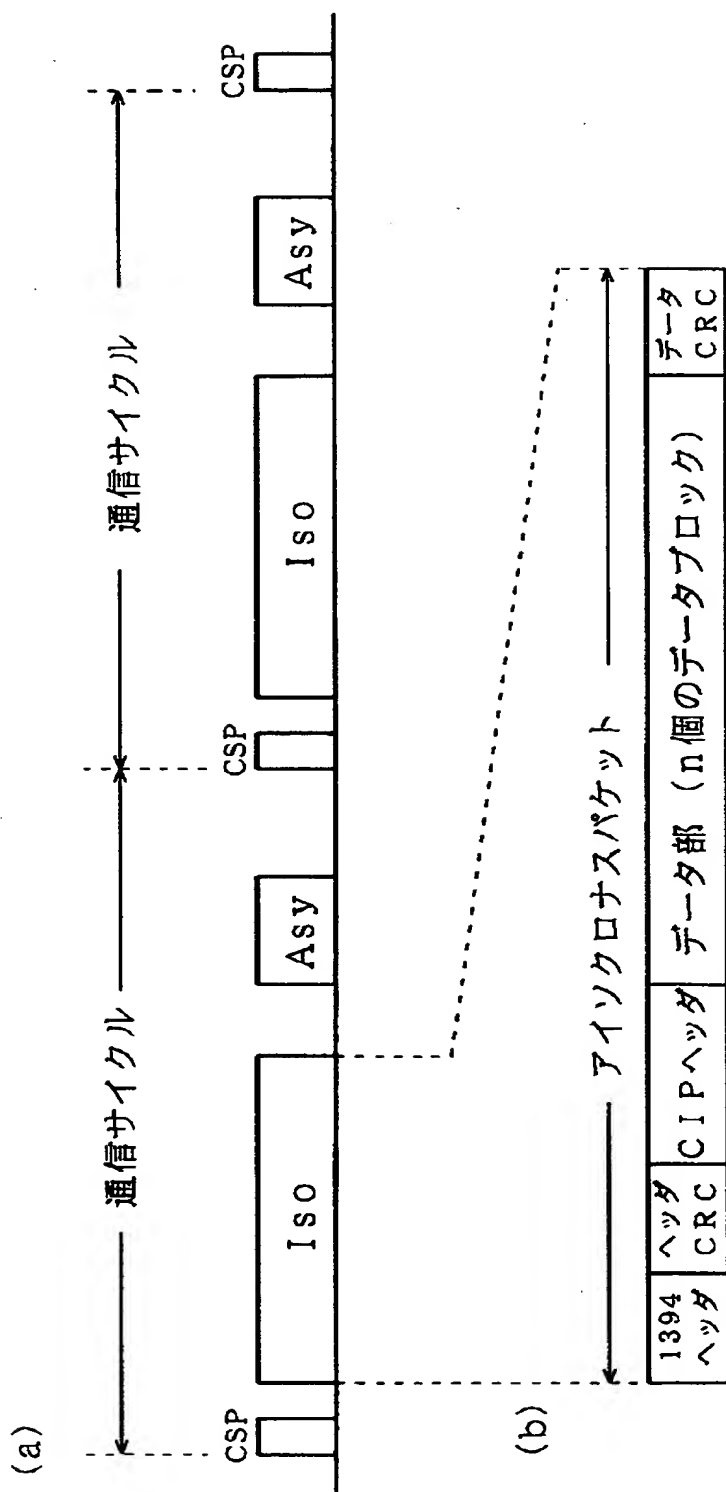
1 送信装置、2 受信装置、3 伝送路、4 記録装置、5 再生装置、6  
メディア、10, 46 ブロック処理部、11, 41 ランダムデータ付加部  
、12, 42 暗号化部、13 送信部、21 受信部、22, 52 復号部、  
23, 53 ブロックデコード部、43 送出部、51 取込部

【書類名】 図面

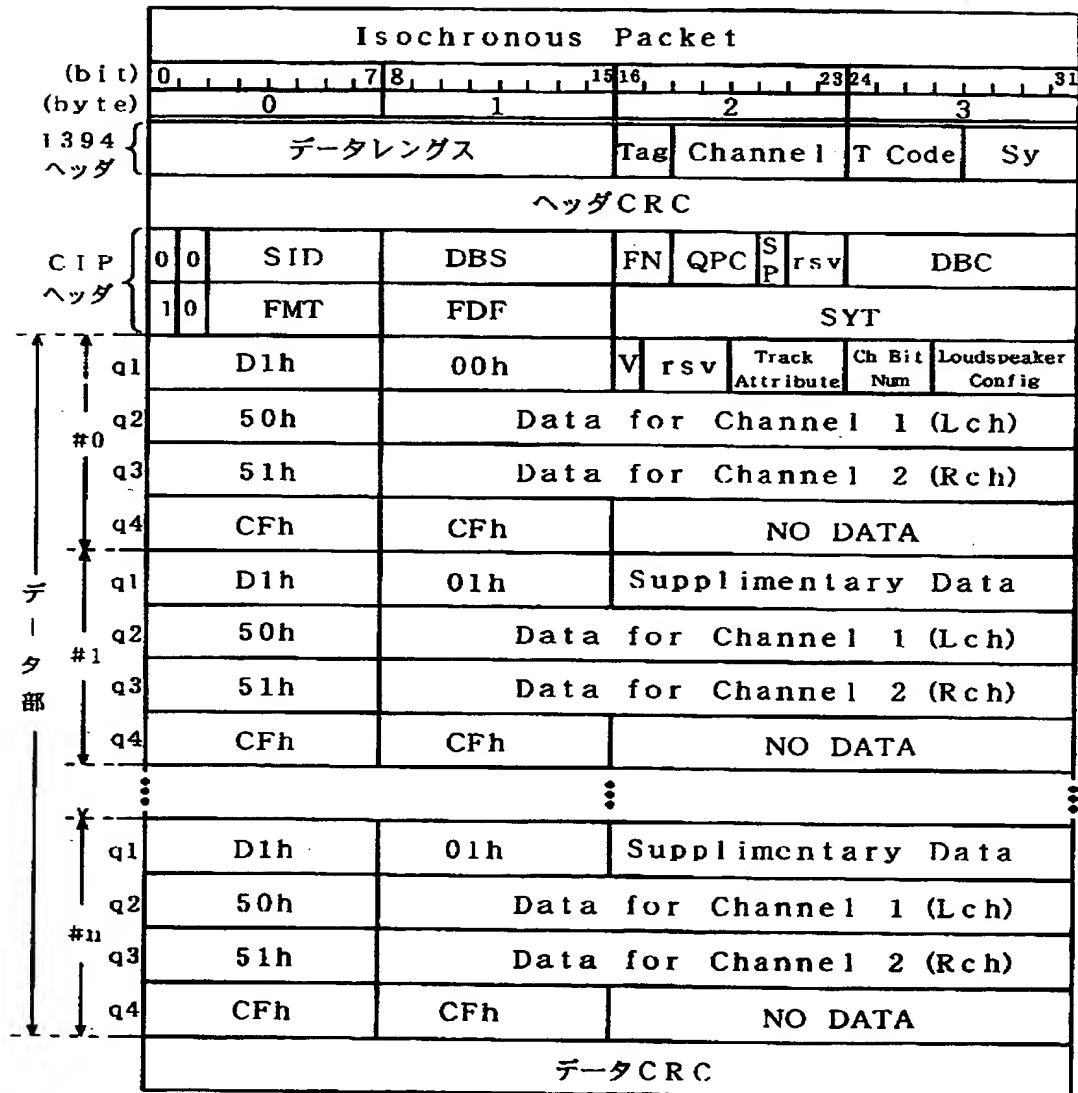
【図1】



【図 2】



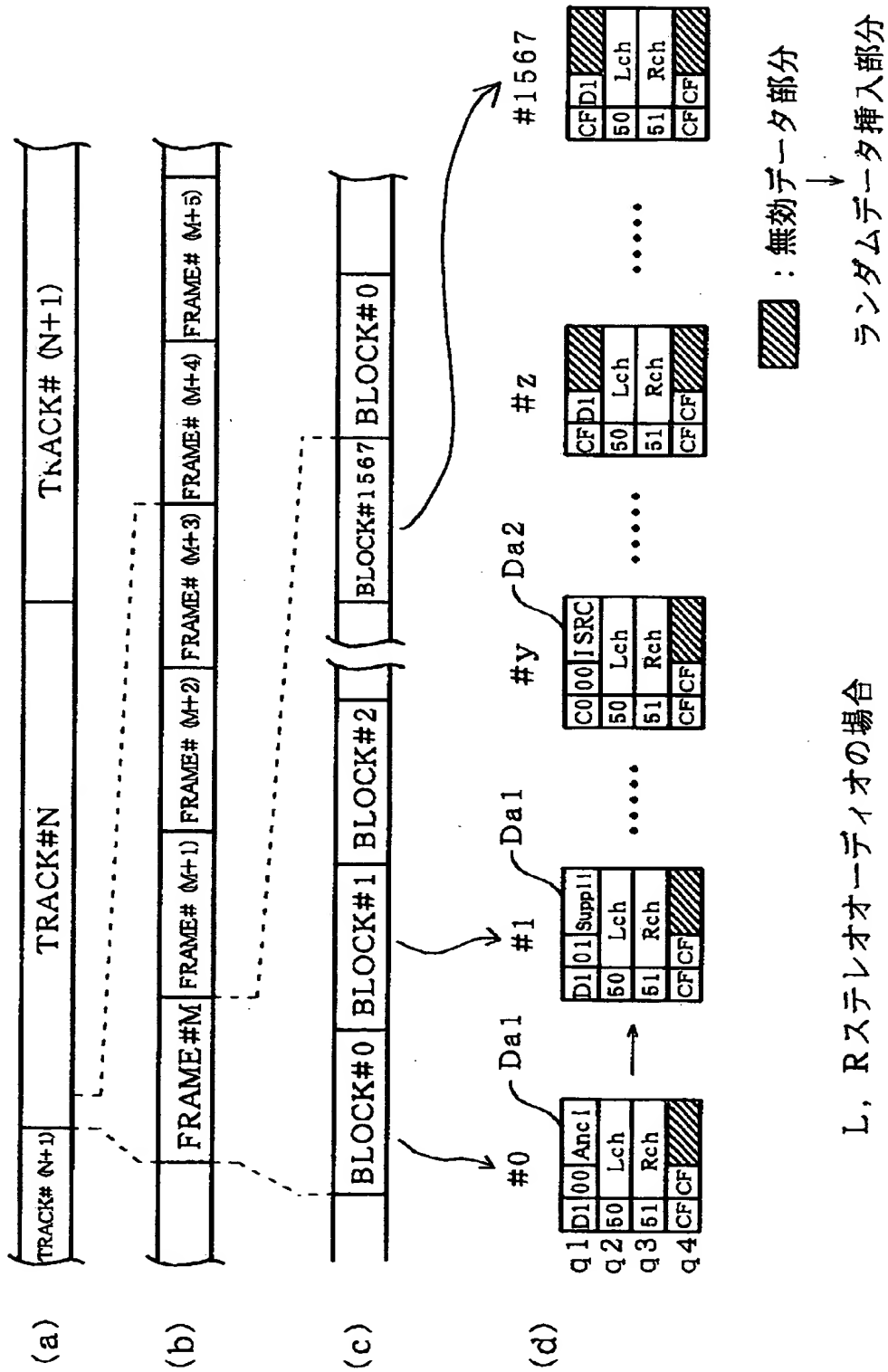
【図 3】



【図4】

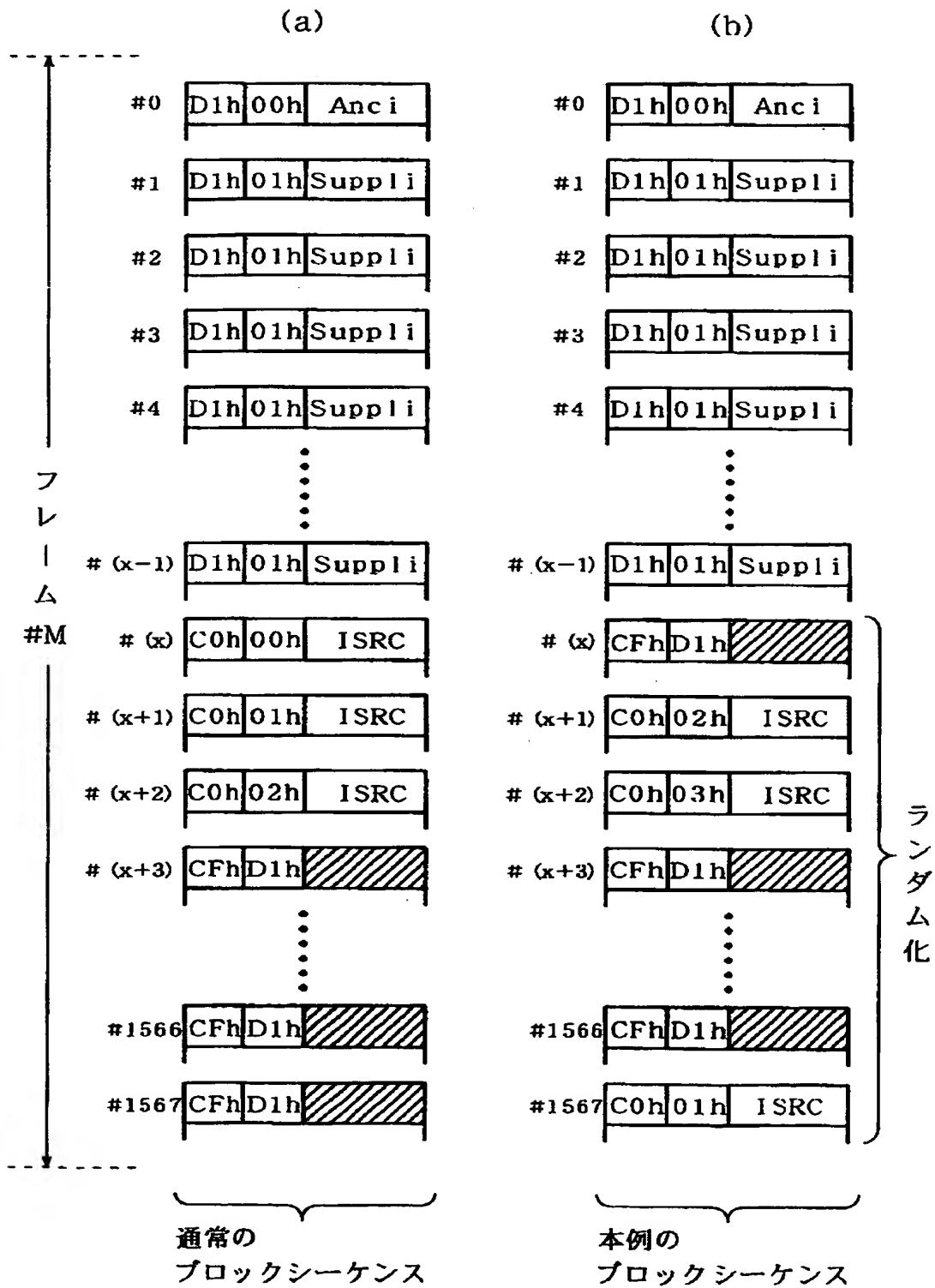
Value	Description
00h-3Fh	IEC60958 Conformant
40h-4Fh	Multi-bit Linear Audio
50h-57h	One Bit Audio (Plain)
58h-5Fh	One Bit Audio (Encoded)
60h-7Fh	-reserved-
80h-83h	MIDI Conformant
84h-87h	Extended Music Data
88h-8Bh	SMPTE Time Code Conformant
8Ch-8Fh	Sample Count
90h-BFh	-reserved-
C0h-EFh	Ancillary Data
F0h-FFh	-reserved-

【图 5】

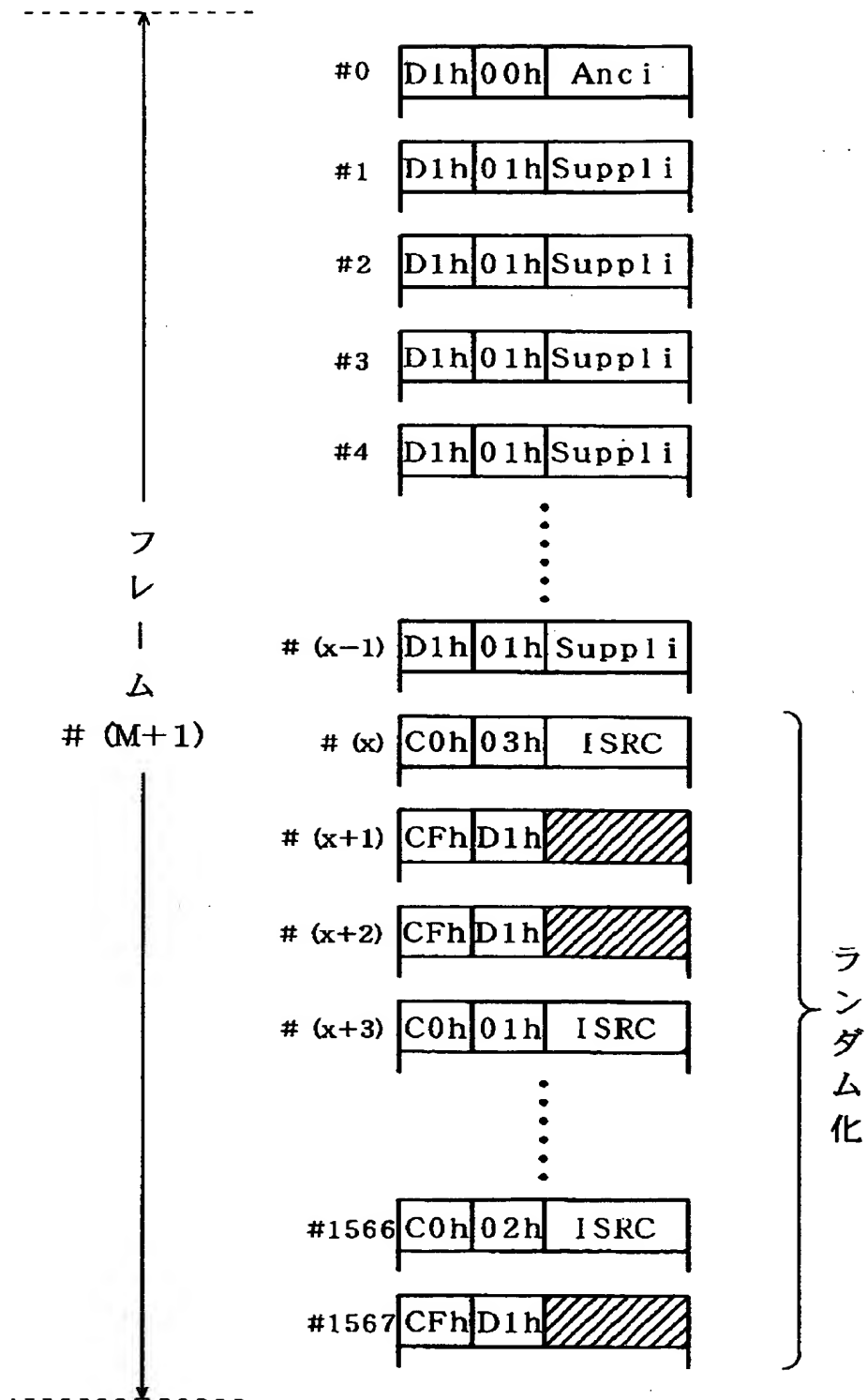


L, Rステレオオーディオの場合

【図 6】

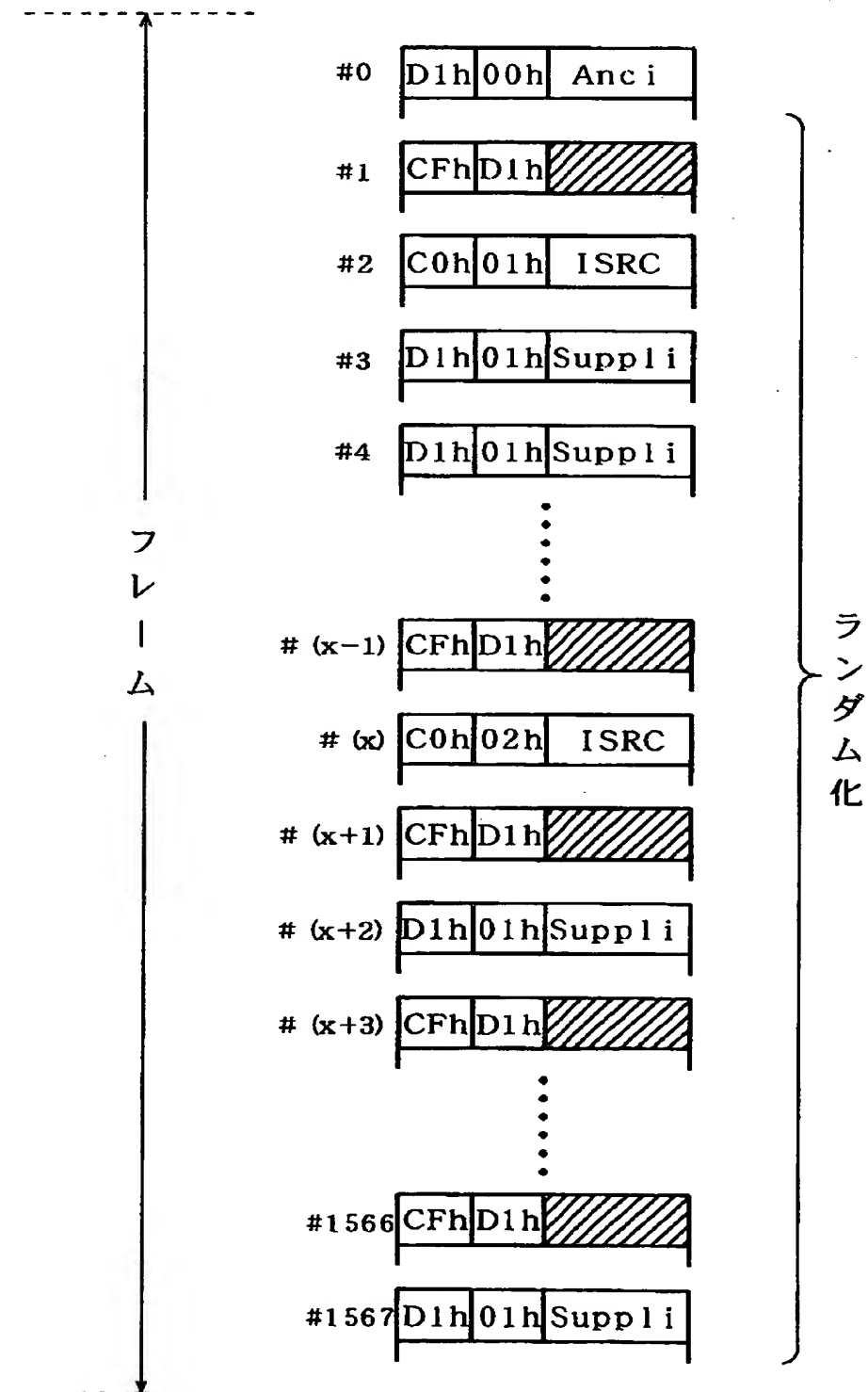


【図 7】

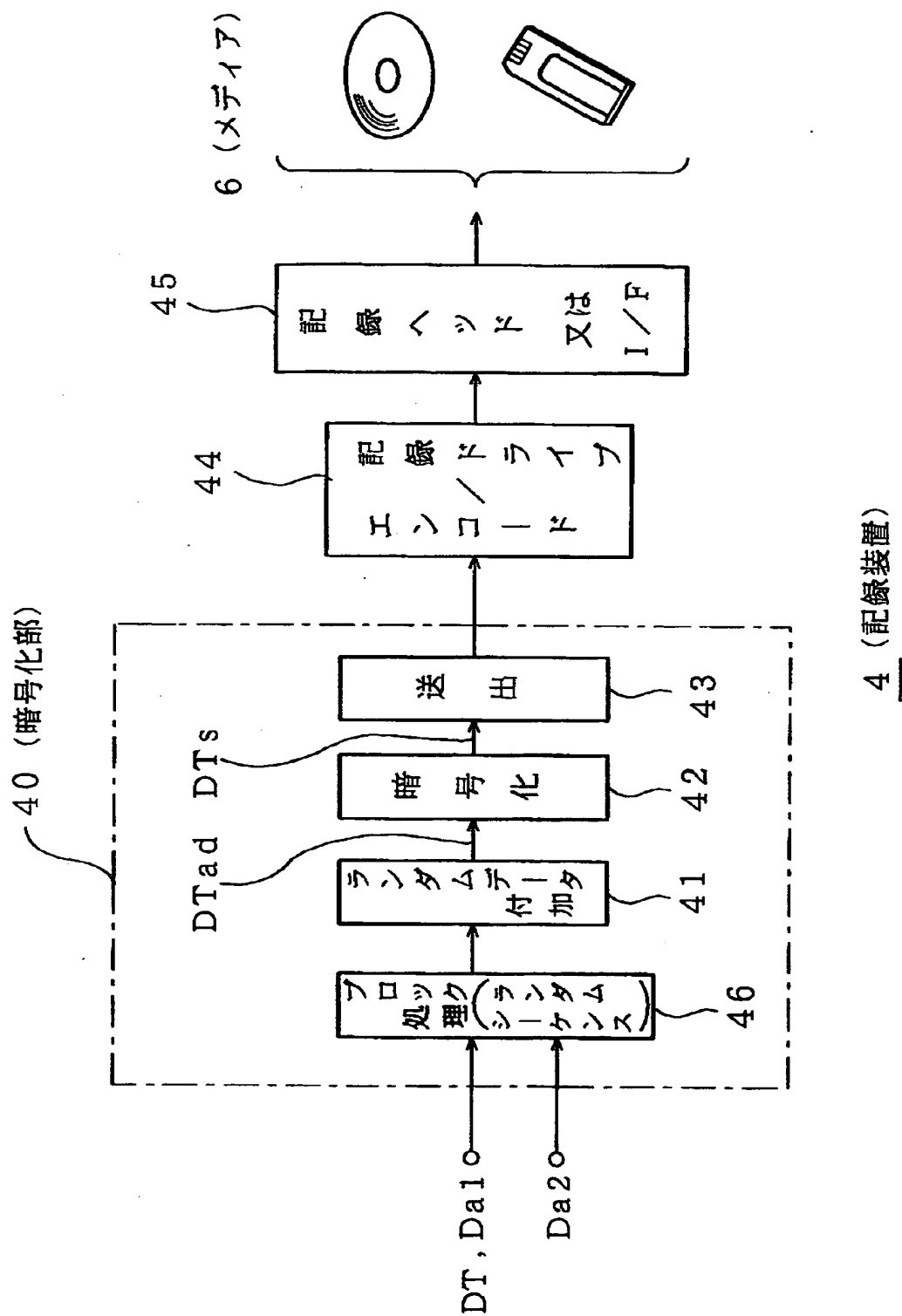




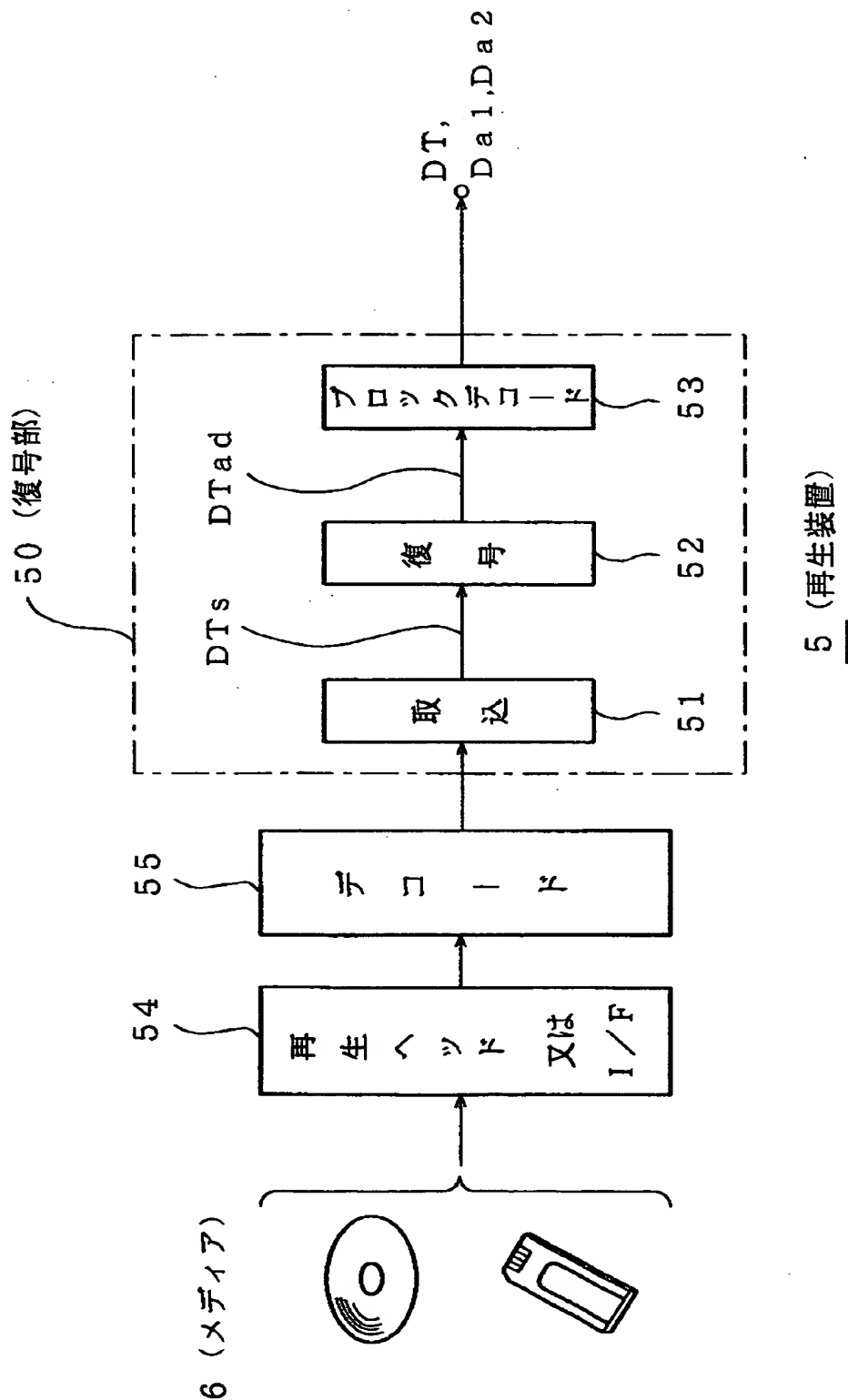
【図 8】



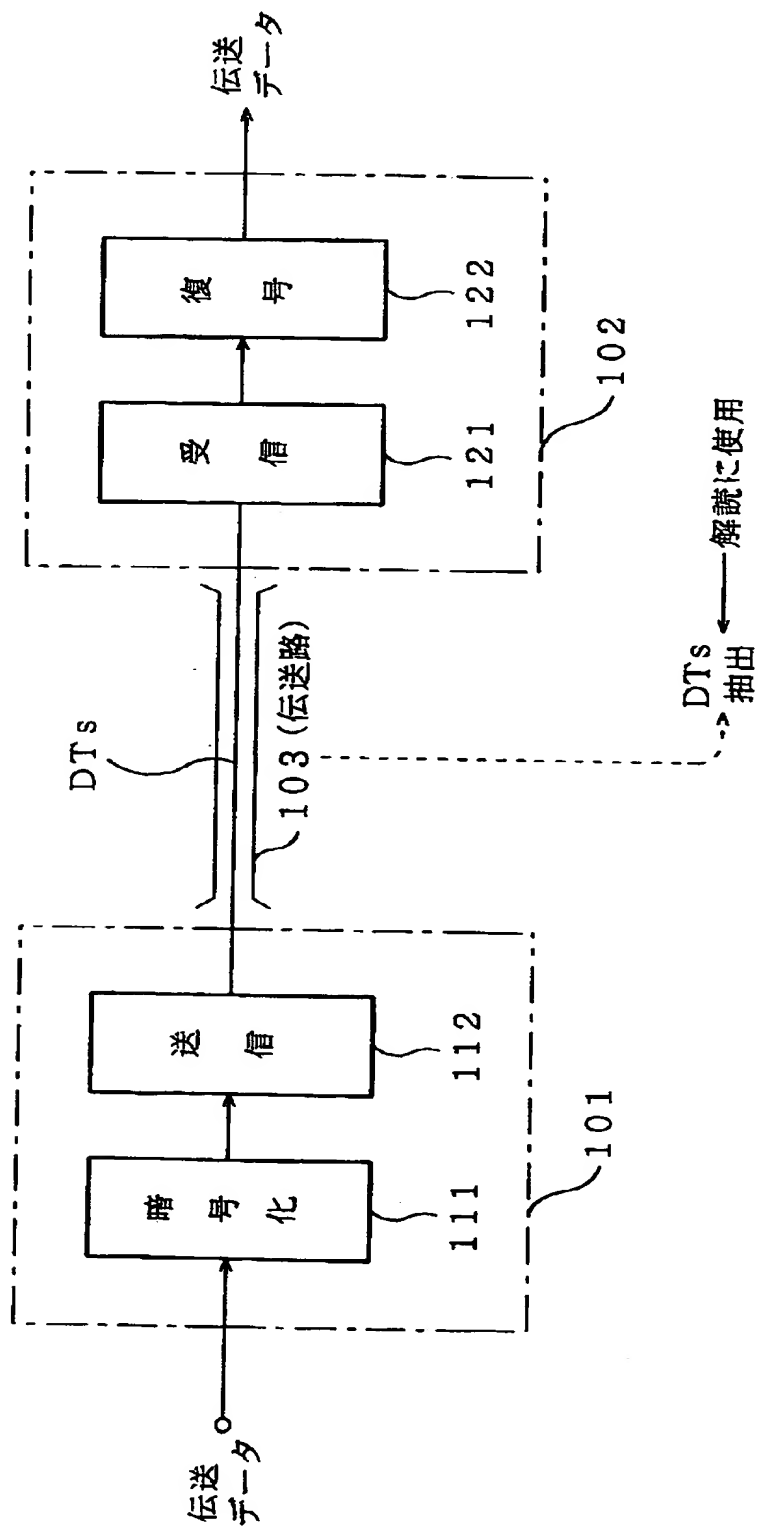
【図9】



【図10】



【図 11】



【書類名】 要約書

【要約】

【課題】 暗号解読が困難で著作権保護などに好適なデータ伝送の実現。

【解決手段】 伝送するデータとしての連続したデータブロックに対して、付加データをランダムに選択したデータブロックに付加することで、付加データが付加される位置が連続するデータブロック内でランダムなものとなるようにしている。これによって、伝送されている暗号化データにおいて、「元の内容が明白なデータ」が配されている位置がわからないようにし、暗号アルゴリズムの解読を困難にする。

【選択図】 図 6

認定・付加情報

特許出願の番号	特願 2 0 0 0 - 2 6 4 5 . 0 6
受付番号	5 0 0 0 5 0 4 4 6 0 4
書類名	特許願
担当官	塩崎 博子 1 6 0 6
作成日	平成 1 2 年 9 月 4 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号
【氏名又は名称】	ソニー株式会社

【代理人】

申請人

【識別番号】	100086841
【住所又は居所】	東京都中央区新川 1 丁目 2 7 番 8 号 新川大原ビル 6 階
【氏名又は名称】	脇 篤夫

【代理人】

【識別番号】	100114122
【住所又は居所】	東京都中央区新川 1 丁目 2 7 番 8 号 新川大原ビル 6 階 脇特許事務所
【氏名又は名称】	鈴木 伸夫

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社